Section 3.4 User Account Administration and Distribution Lists

User Account Administration

Creating New User Accounts

When a request is received to create a new user account, the agent first checks the Entire Directory to ensure the user account does not already exist. If the account exists, a comparison is made of the existing account's properties with the information on the new request to determine if it is a duplicate. Notification is returned to the requestor if evidence reflects it is a duplicate request.

After connecting to the correct domain and domain controller, an agent selects the correct Claimant OU, then the correct Base OU. The agent then creates a unique account, using naming standards to differentiate users with the same name. If the account is for a foreign national, the naming standards also require a country code. An Exchange mailbox is then created.

Modifying Existing Accounts

A user name may be changed in Active Directory. After ensuring that the user is not logged on to the network, the agent connects to the correct domain and domain controller and locates the user's name. The correct file server is noted from the user's profile. Using terminal serves, the agent connects to the file server and appropriate folder. The user's name is changed and a notation made in the shared properties. Once the change is made and the connection to the local file server is closed, Active Directory is updated to reflect the new name. Next, the change is propagated to the user's email address. User properties are also updated to reflect the change. When all steps are completed, the customer is contacted and told to wait approximately 30 minutes before logging on with the new name.

Requests for changes to profile properties follow many of the same procedures.

Asset Assignments

A request to assign an asset to a user requires an existing user account. After locating the user name on the domain, the agent opens NVDUSrMgr and locates the machine name. After reviewing the list of users bound to the machine, the agent adds the user and the user's login name. A similar update is made in the Remedy Asset Record where the asset ID is added and in the People Record to update the person role. In most cases, the ticket is then assigned to base Ops for completion. When notification is received that the request is complete, a reply email is sent to the requestor.

Deleting Accounts

Active Directory accounts may be deleted or inactivated. After connecting to the correct domain and domain controller, the agent locates the correct account, and notes the new action and the ticket number.

If the request is to inactivate an account, group memberships are not deleted. An update is made to the user name to indicate it is in inactive status. Requests to delete an account, group memberships are removed except Domain Users.

If an Asset Number is provided with the request, an additional step of Asset Unassignment is performed. When it is not provided, several searches are performed to locate it. When located, the user's name is removed from the asset.

Distribution Lists

Creation

A CTR's request to create a distribution list in Active Directory requires that the user has an NMCI account. After connecting to the correct domain and domain controller, an agent selects the correct Claimant OU, then the correct Base OU. When creating the new group, the group names must comply with the NMCI naming standards. With the group created, the distribution list is created using the same group name. Members are added, a list owner assigned, and security properties granted in the final steps of the process.

Administration

Changes to a distribution list occur when new members are added or existing members are deleted. After connecting to the correct domain and domain controller, the agent selects the distribution list name. Users can be added individually or selected from the list. Similarly, users can be removed from a distribution list.